16869P-018300US
Chun-Pok Leung, Reg. No. 41,405
Telephone: 650-326-2400
Title: Method and System for Recovering the.....
Inventors: Kunihiko Miyazaki et al.
Sheets of drawings 1 of 18

FIG. 1
PRIOR ART

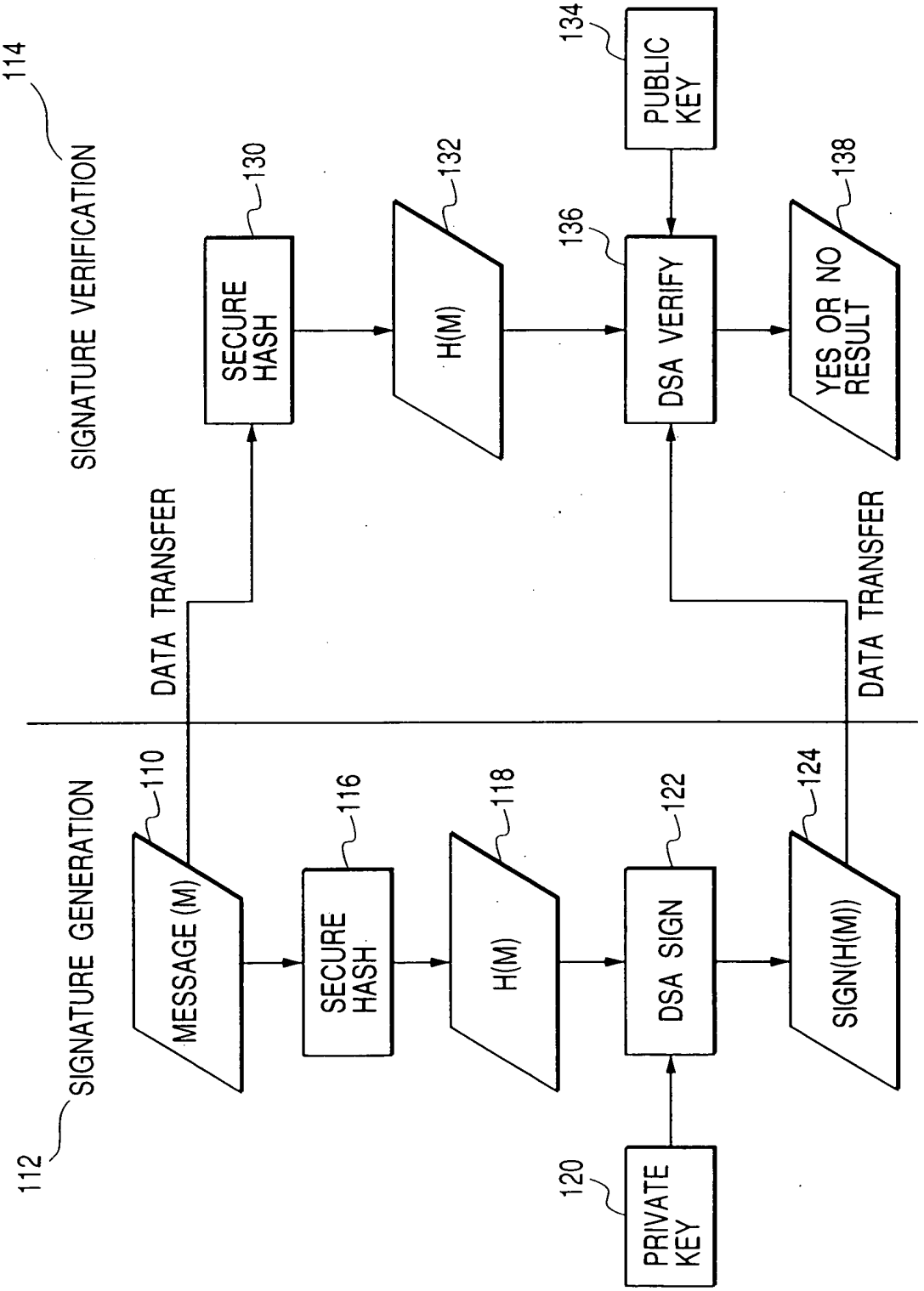


FIG. 2

VALIDITY RECOVERY SYSTEM

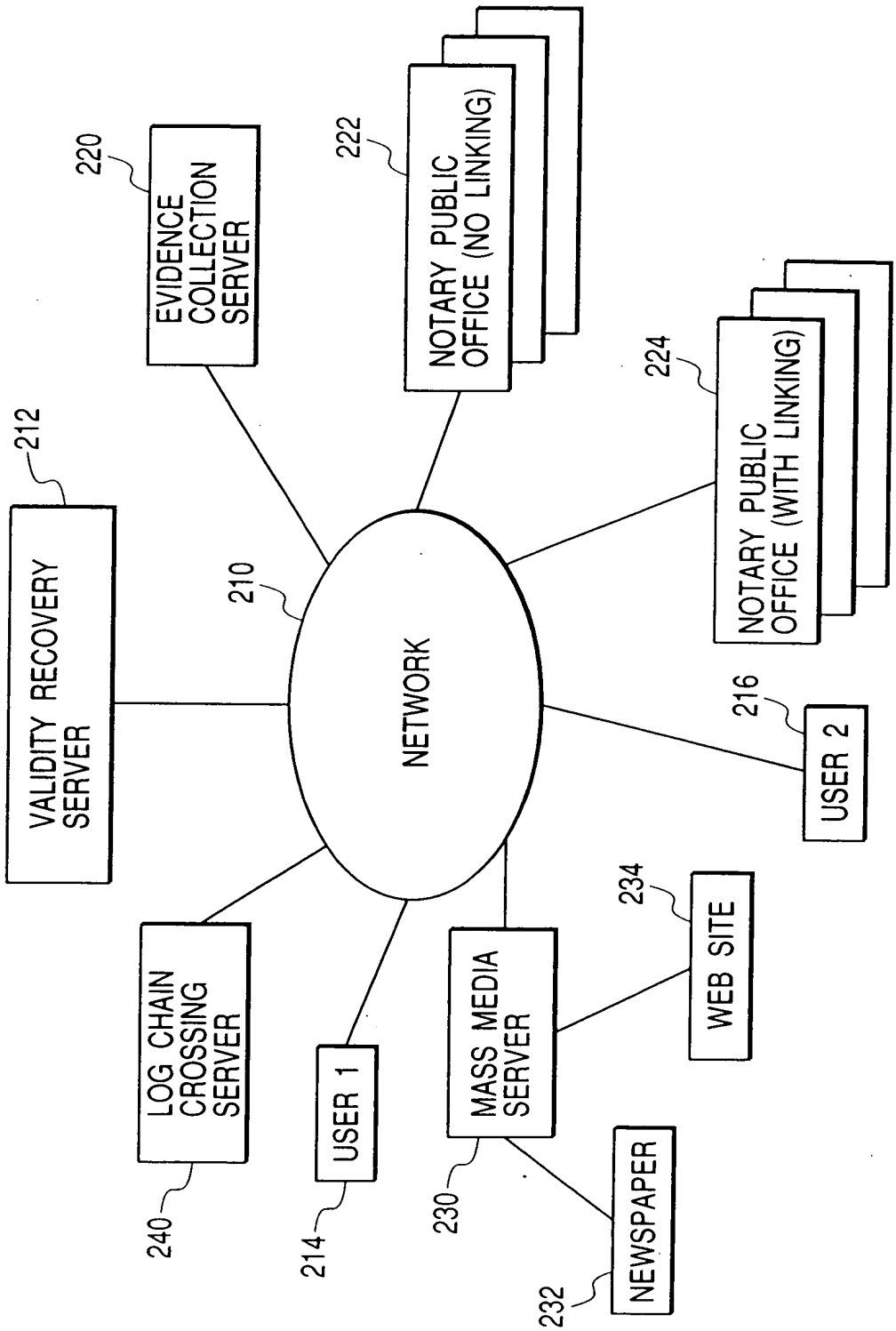


FIG. 3

EXAMPLE COMPUTER

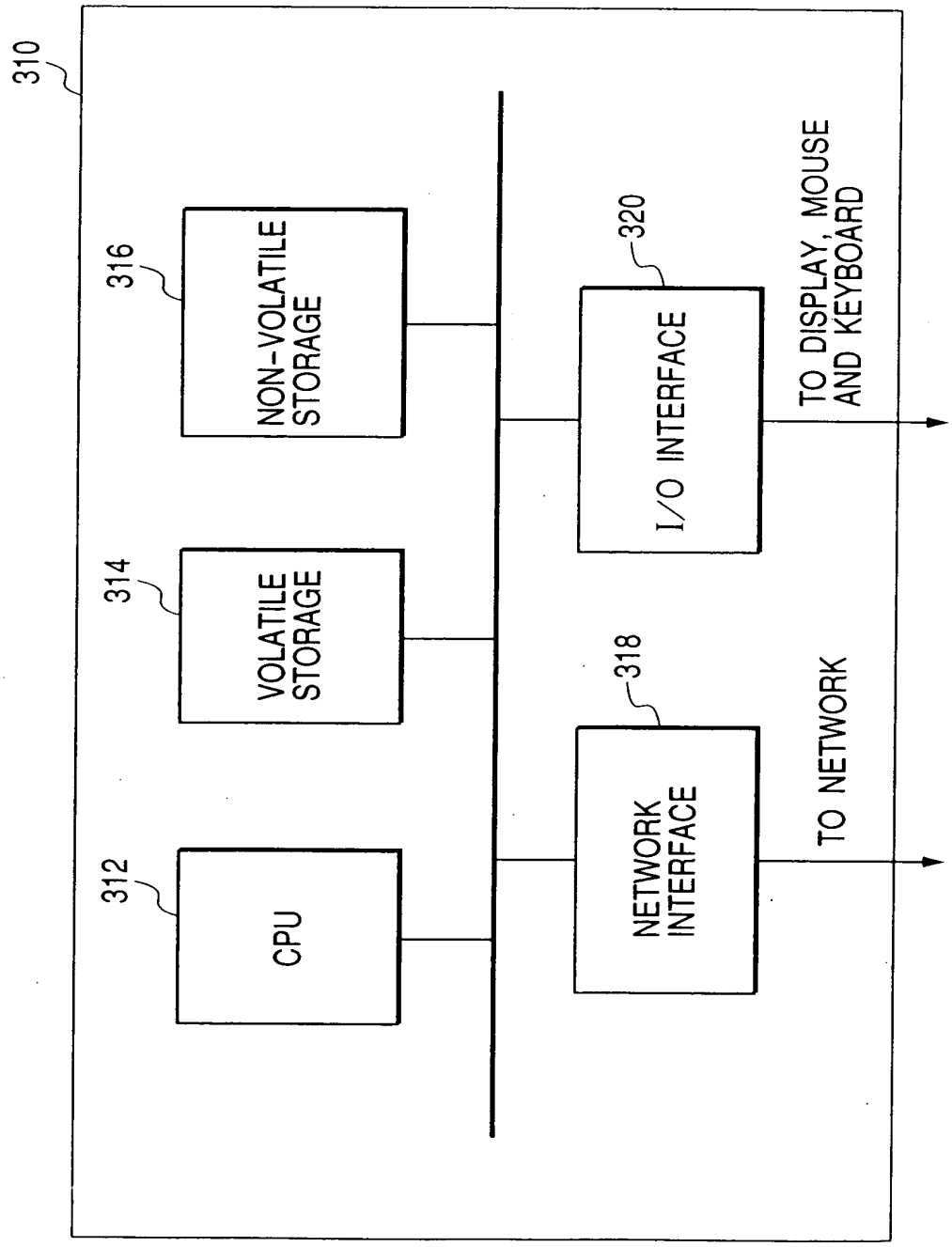


FIG. 4

MESSAGE FORMAT (410)

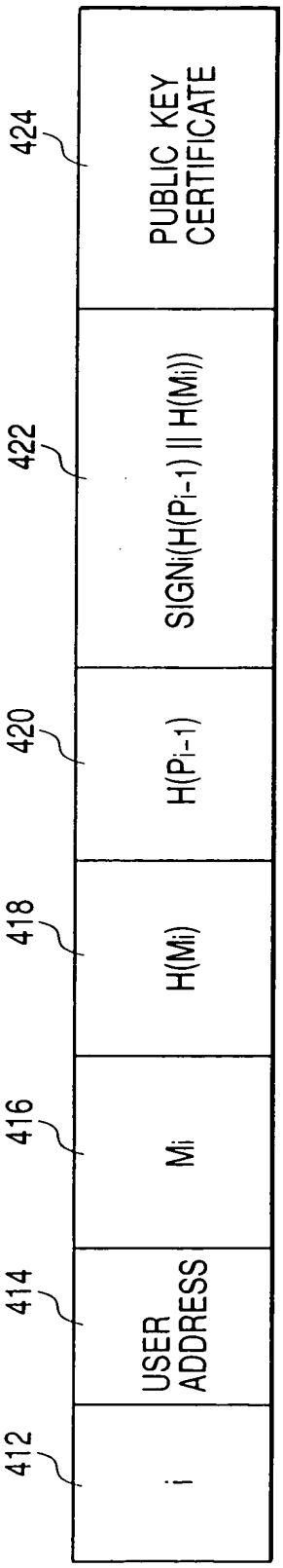


FIG. 5

MESSAGE FORMAT WITH TIMESTAMP (510)

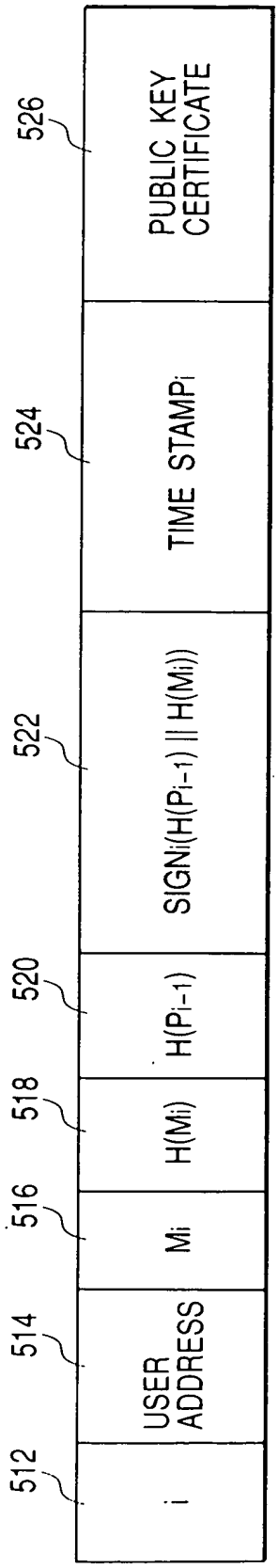


FIG. 6

SIGNATURE LOG

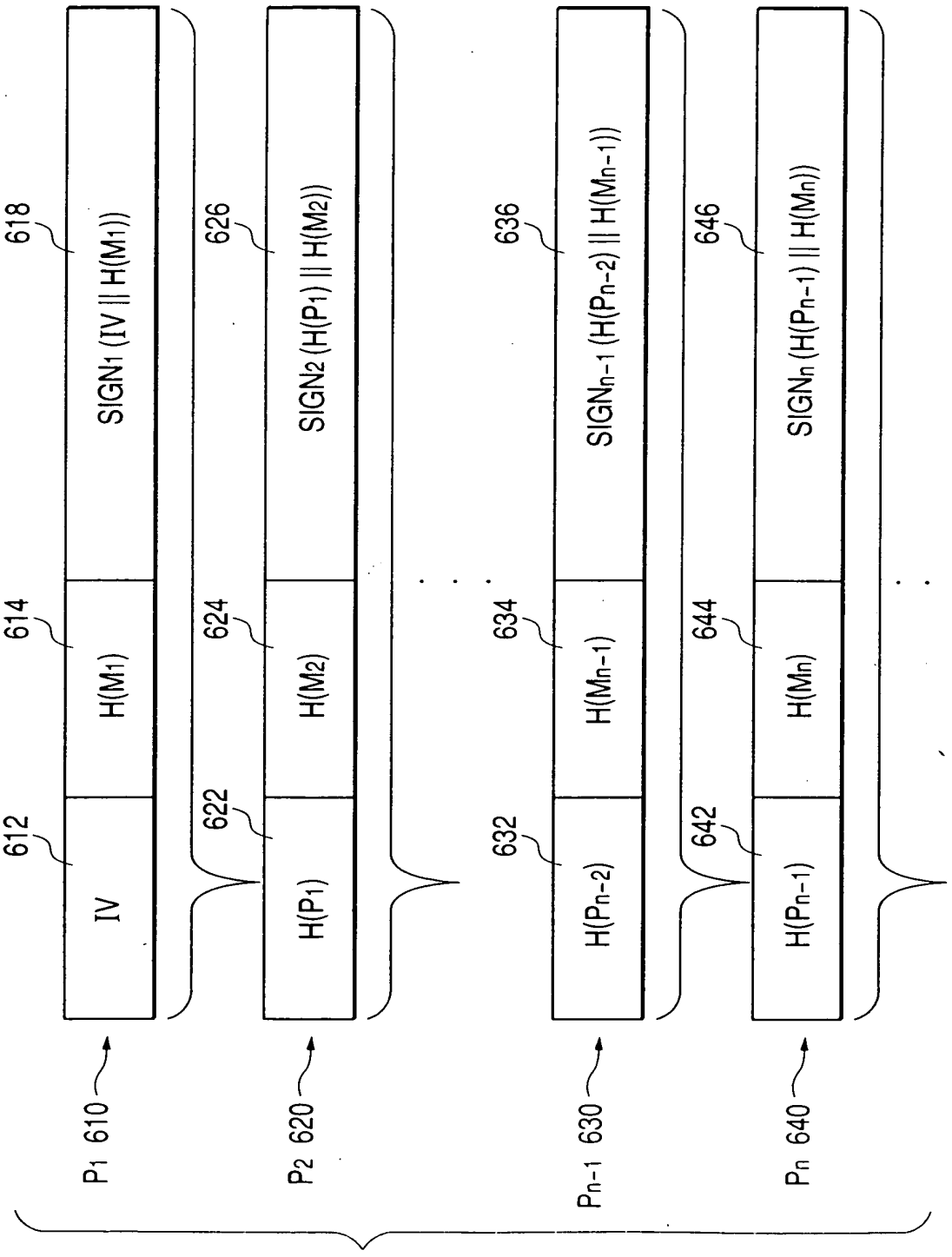


FIG. 7

ANOTHER SIGNATURE LOG WITH TIMESTAMP

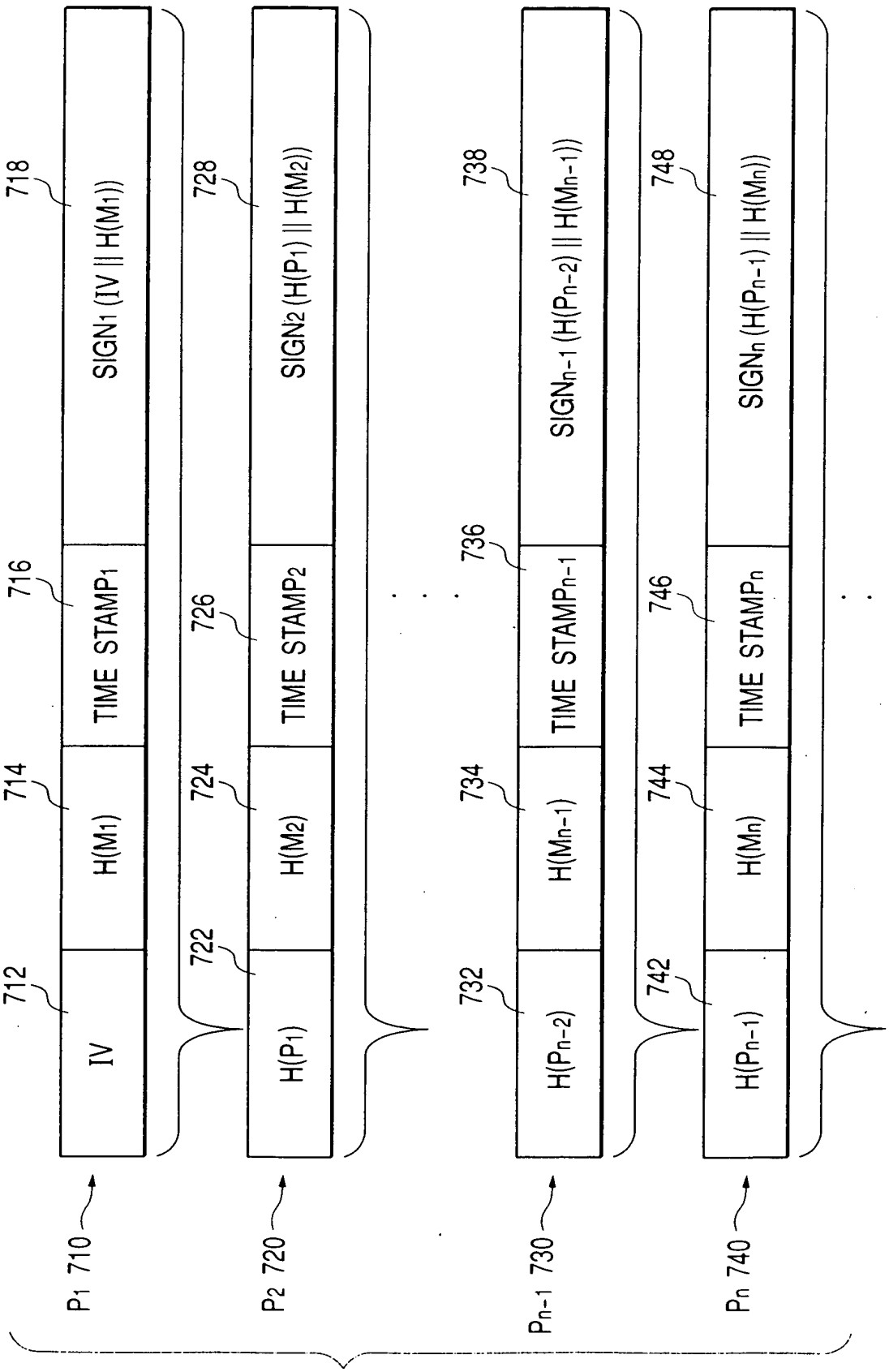


FIG. 8

VALIDATING LOG ENTRIES-BACKWARD CHAINING

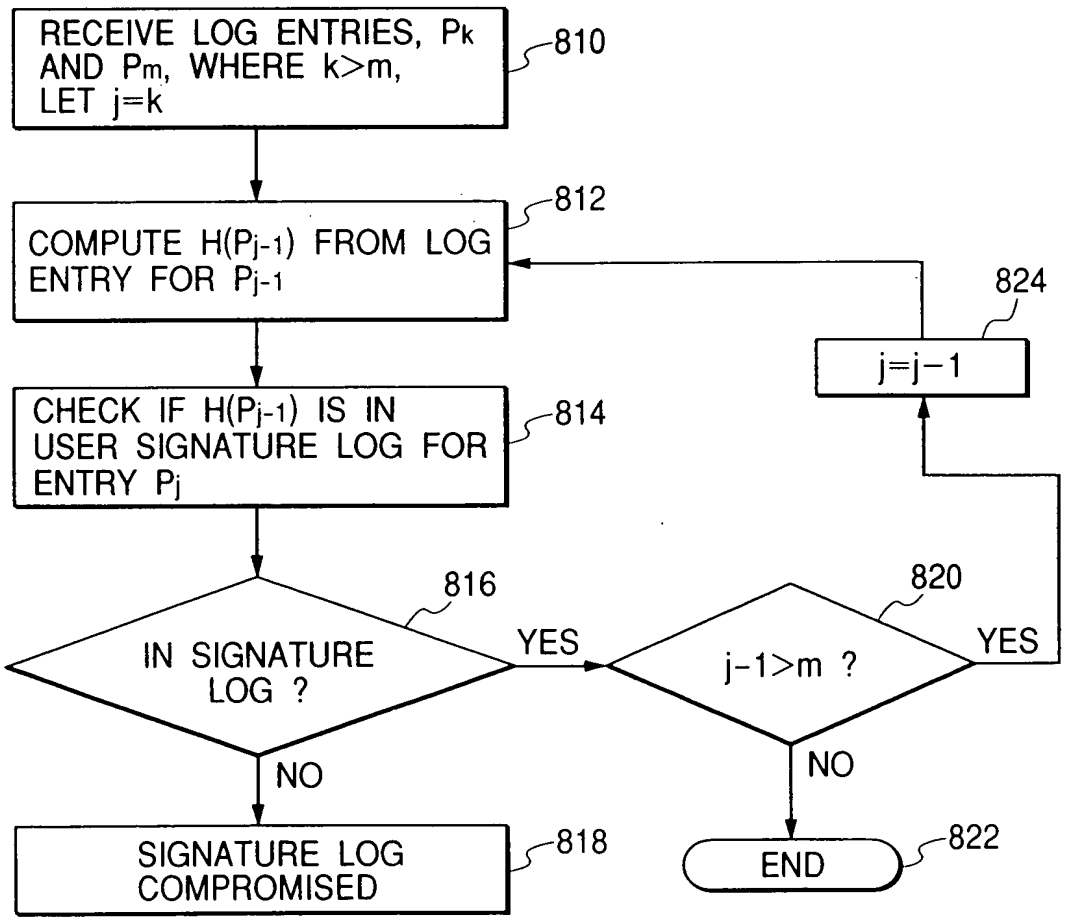


FIG. 9

CHECKPOINTING (e.g.,PUBLISHING OR NOTARY) LOG ENTRY

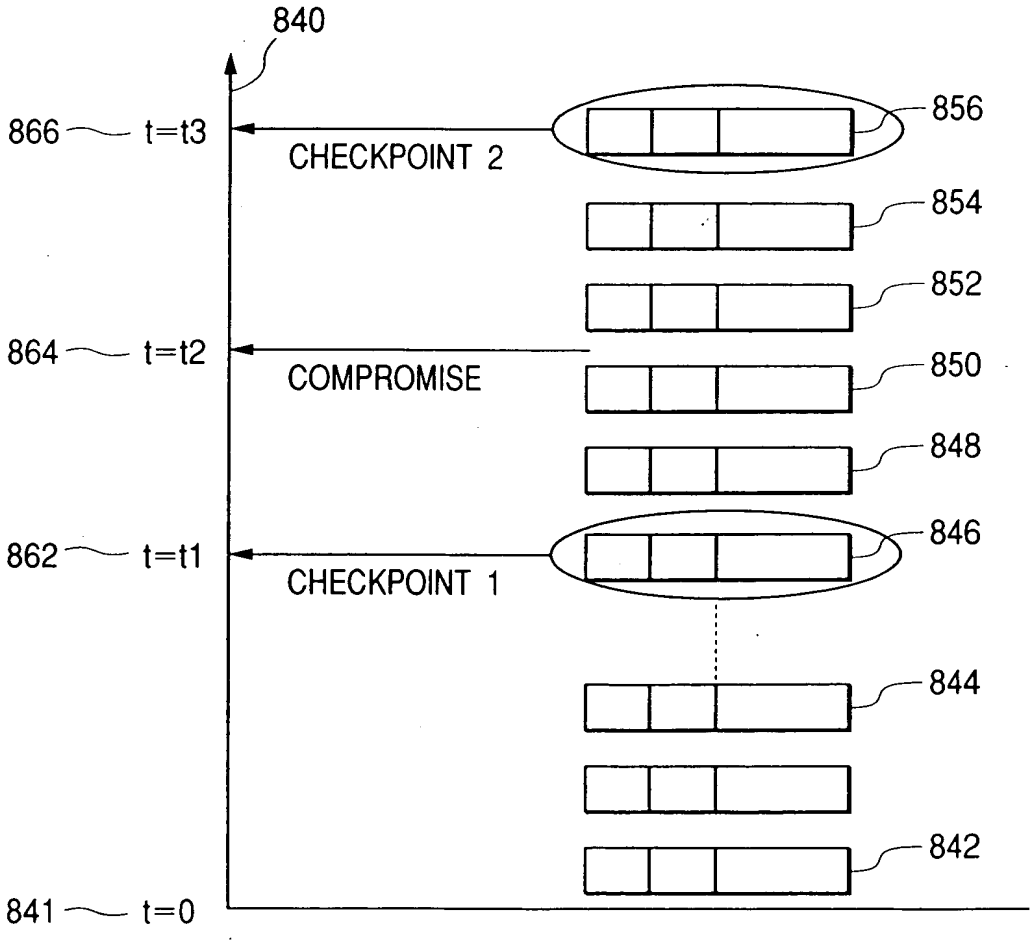


FIG. 10

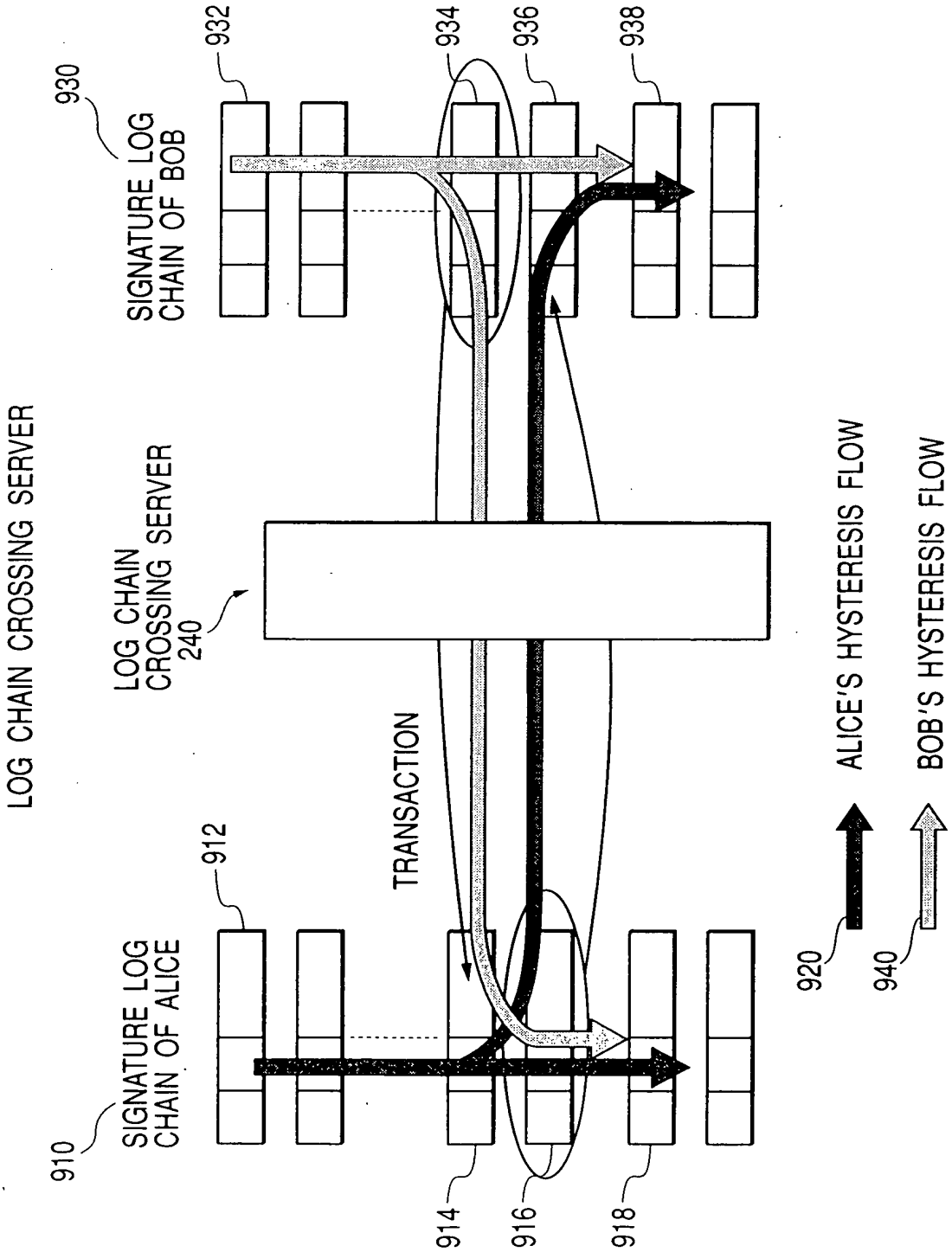

LOG CHAIN CROSSING SERVER
930
SIGNATURE LOG CHAIN OF BOB
932
934
936
938
LOG CHAIN CROSSING SERVER
240
TRANSACTION
912
910
SIGNATURE LOG CHAIN OF ALICE
914
916
918
ALICE'S HYSTERESIS FLOW
BOB'S HYSTERESIS FLOW
920
940

FIG. 11

NOTARY WITH LINKING

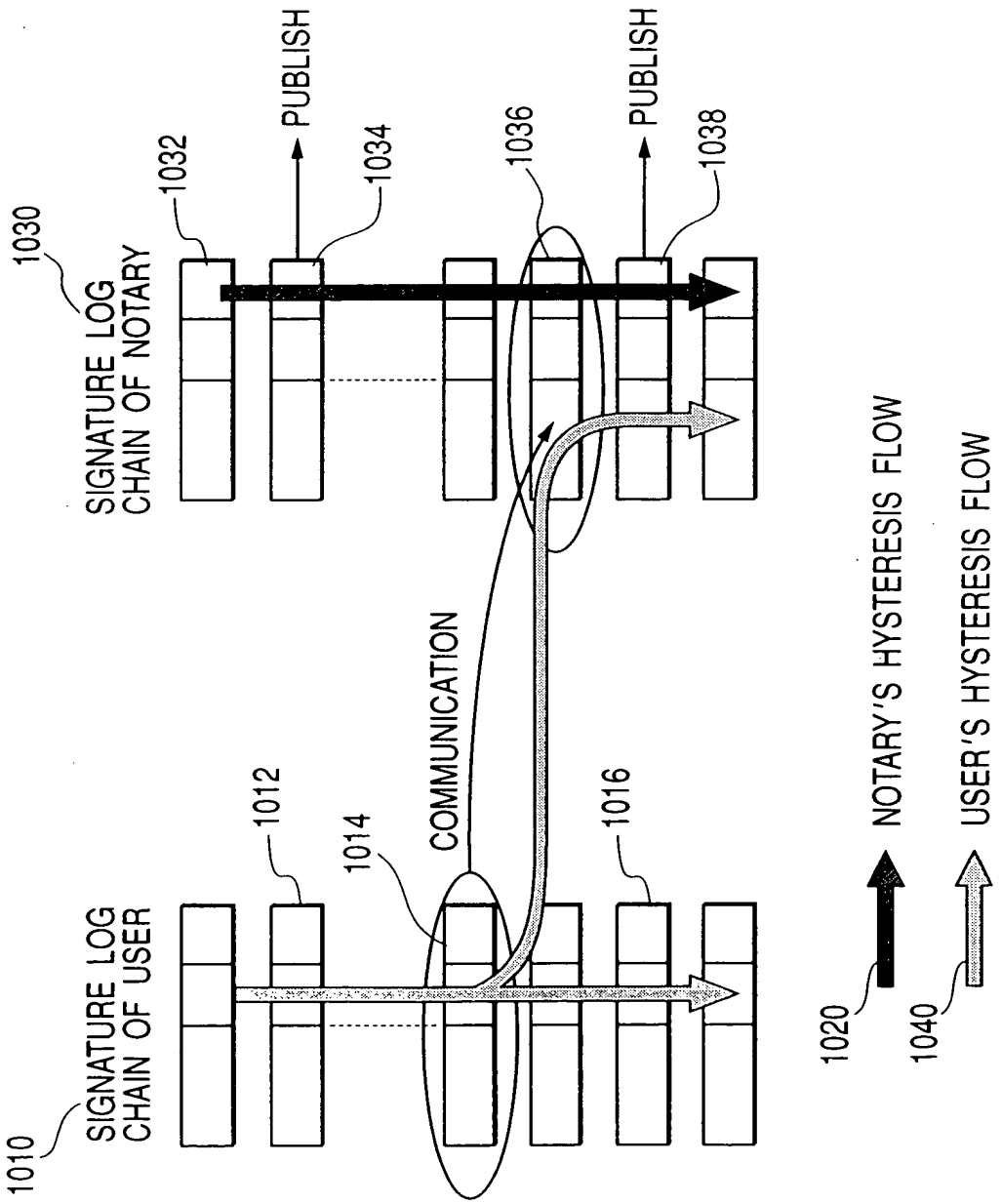


FIG. 12

MASS MEDIA SERVER

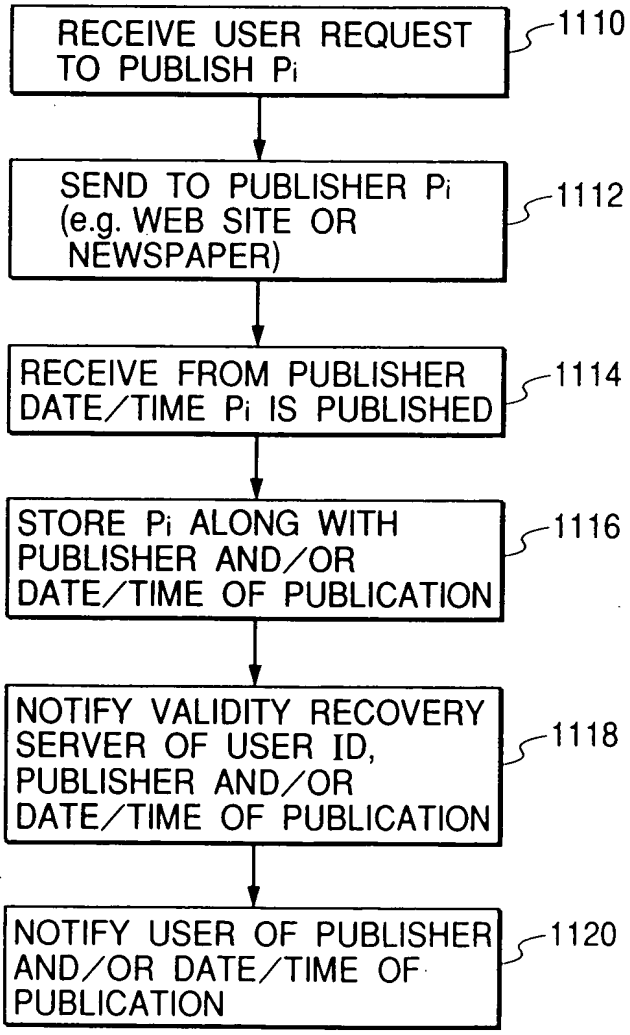


FIG. 13

RECOVERY SERVER DETERMINING IF SIGNATURE LOG ENTRY HAS BEEN CHECKPOINTED

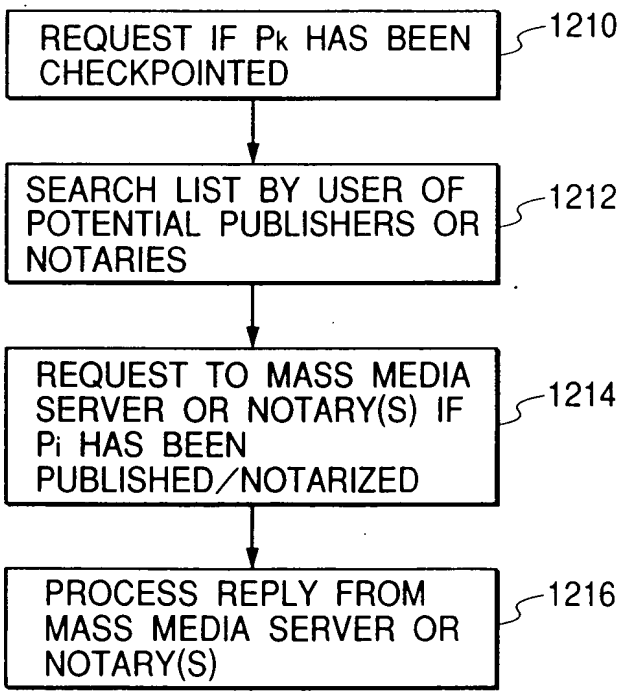


FIG. 14

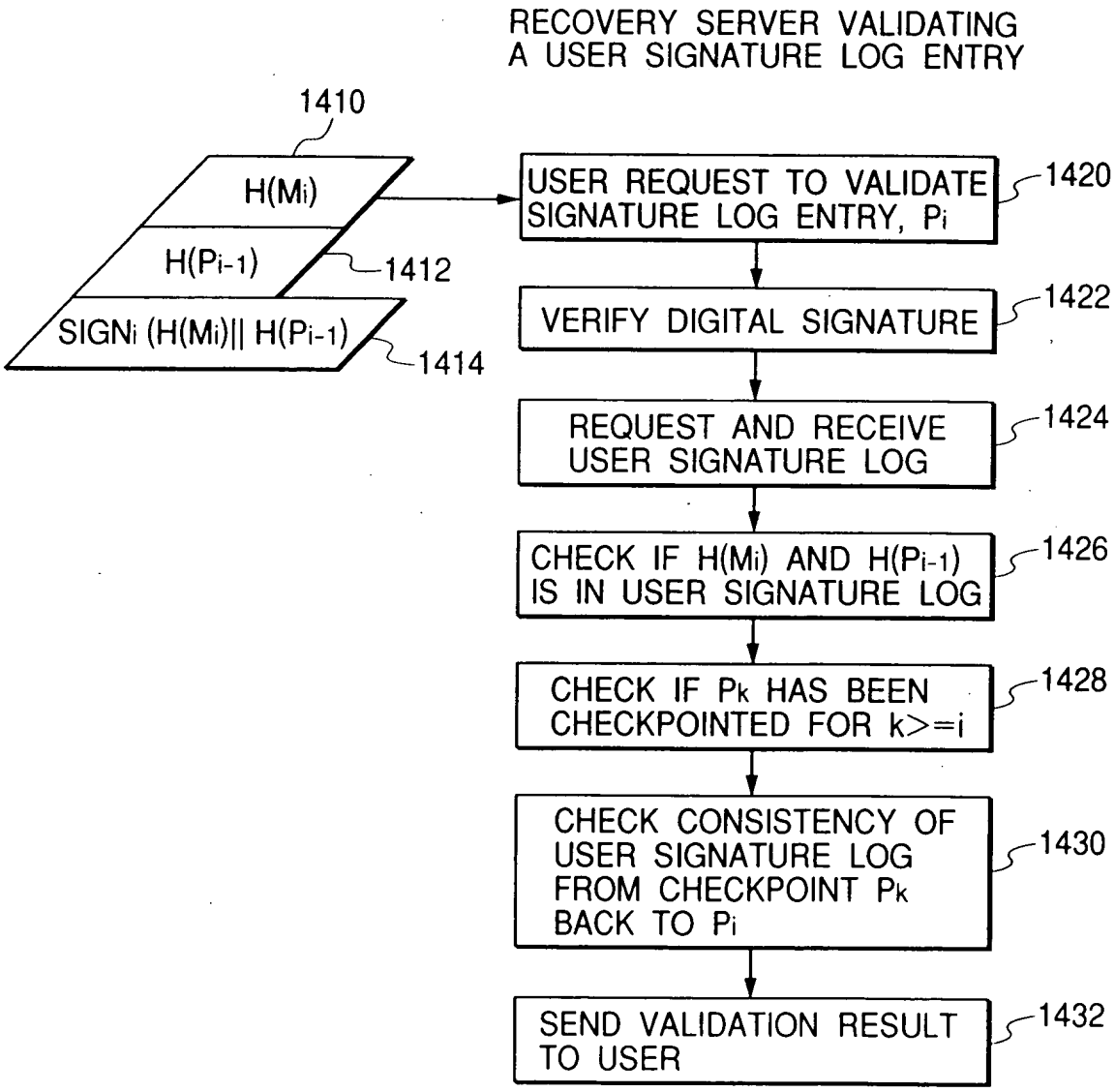

RECOVERY SERVER VALIDATING A USER SIGNATURE LOG ENTRY
1410
H(Mi)
H(Pi-1)
1412
SIGNi (H(Mi)|| H(Pi-1)
1414
USER REQUEST TO VALIDATE SIGNATURE LOG ENTRY, Pi
1420
VERIFY DIGITAL SIGNATURE
1422
REQUEST AND RECEIVE USER SIGNATURE LOG
1424
CHECK IF H(Mi) AND H(Pi-1) IS IN USER SIGNATURE LOG
1426
CHECK IF Pk HAS BEEN CHECKPOINTED FOR k>=i
1428
CHECK CONSISTENCY OF USER SIGNATURE LOG FROM CHECKPOINT Pk BACK TO Pi
1430
SEND VALIDATION RESULT TO USER
1432

FIG. 15

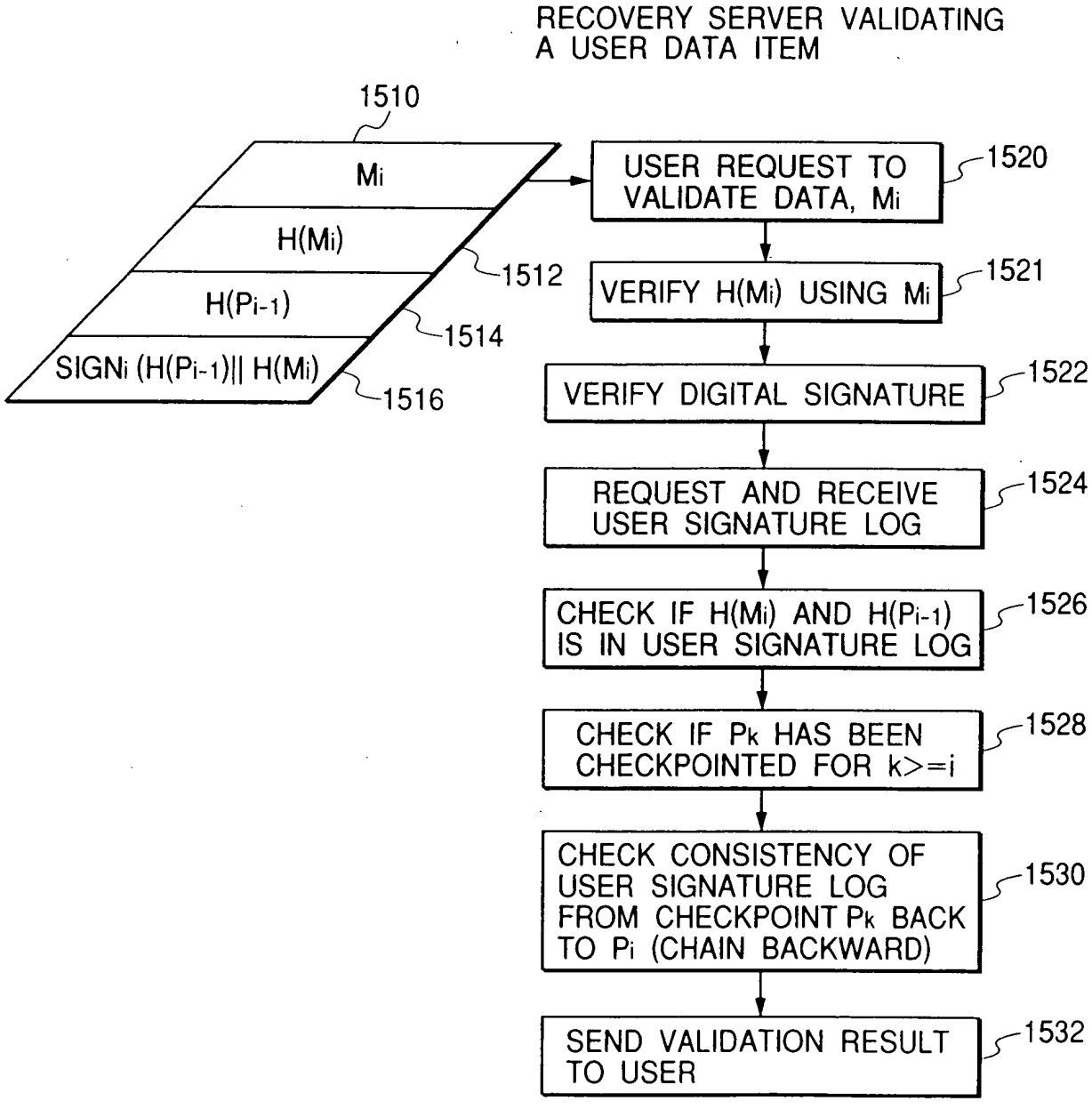

RECOVERY SERVER VALIDATING A USER DATA ITEM
1510
Mi
H(Mi)
H(Pi-1)
SIGNi (H(Pi-1)|| H(Mi)
1512
1514
1516
USER REQUEST TO VALIDATE DATA, Mi
1520
VERIFY H(Mi) USING Mi
1521
VERIFY DIGITAL SIGNATURE
1522
REQUEST AND RECEIVE USER SIGNATURE LOG
1524
CHECK IF H(Mi) AND H(Pi-1) IS IN USER SIGNATURE LOG
1526
CHECK IF Pk HAS BEEN CHECKPOINTED FOR k>=i
1528
CHECK CONSISTENCY OF USER SIGNATURE LOG FROM CHECKPOINT Pk BACK TO Pi (CHAIN BACKWARD)
1530
SEND VALIDATION RESULT TO USER
1532

FIG. 16

EVIDENCE COLLECTION SERVER COLLECTING DATA

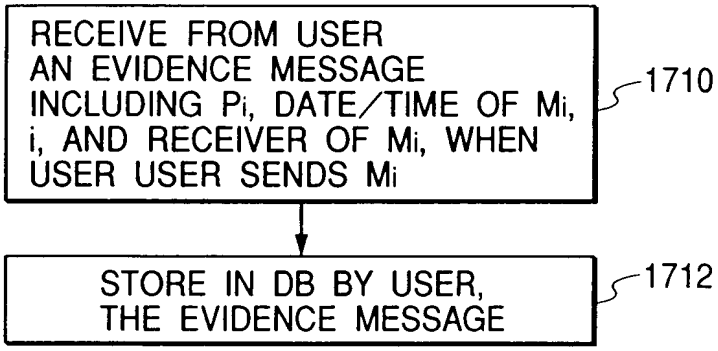


FIG. 17

EVIDENCE COLLECTION SERVER RECOVERING DATA

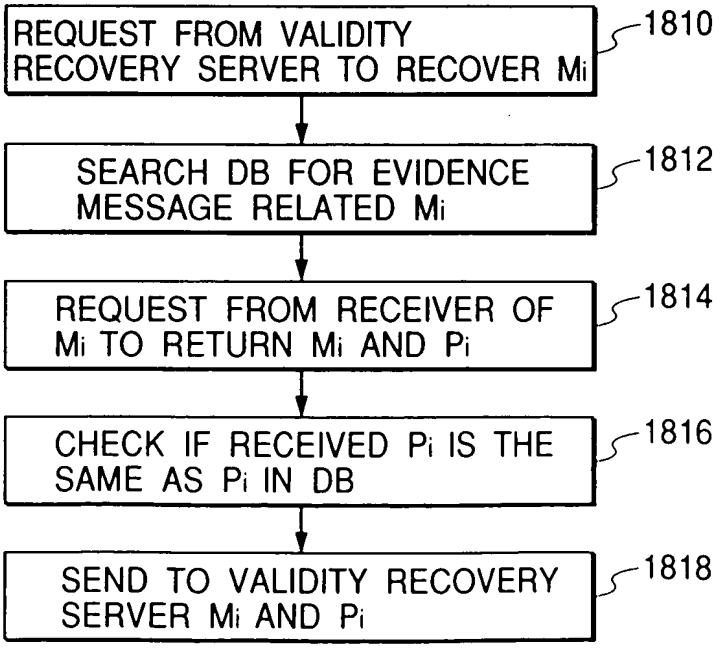


FIG. 18

RECOVERY SERVER RECOVERING USER SIGNATURE LOG ENTRY

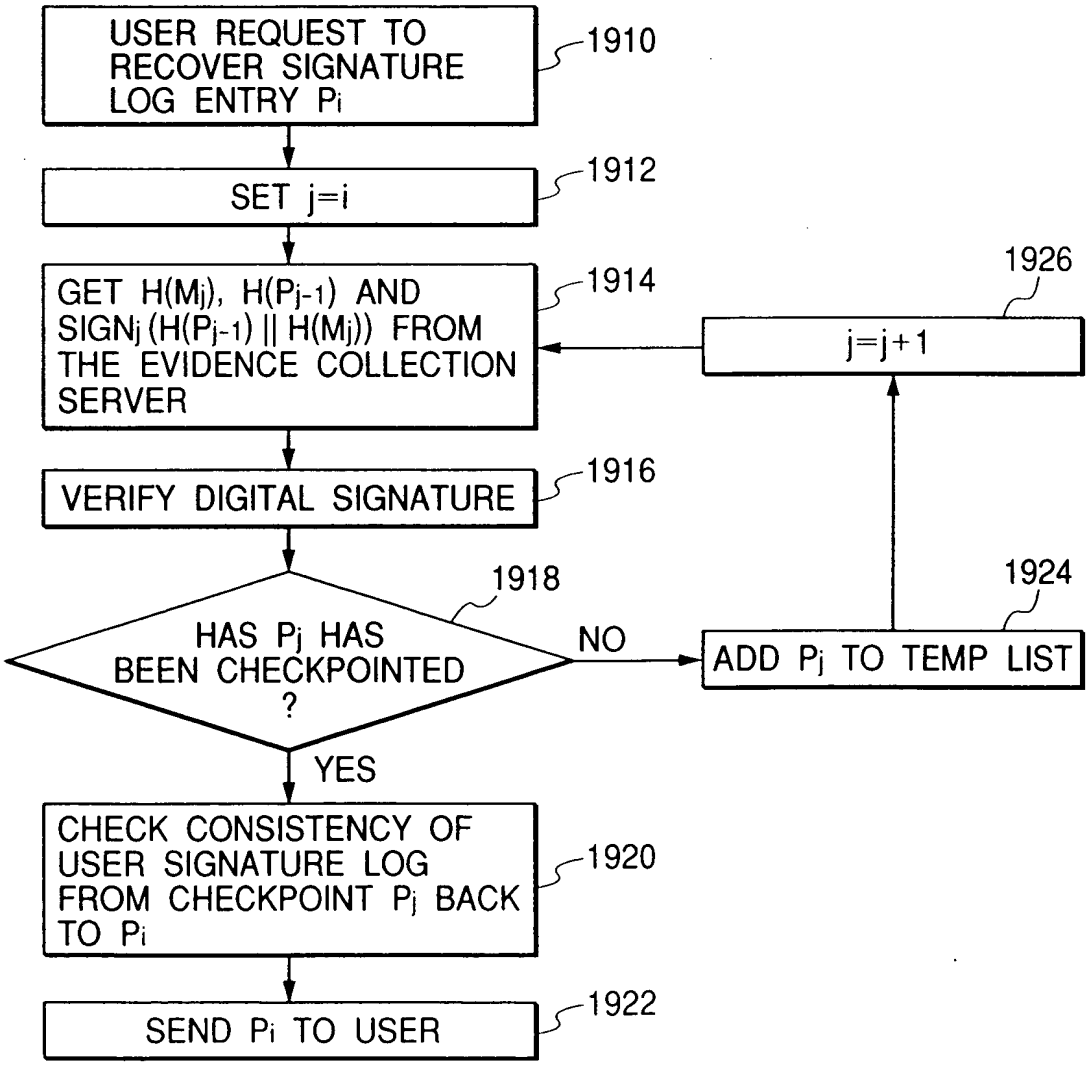


FIG. 19

RECOVERY SERVER RECOVERING USER DATA ITEM

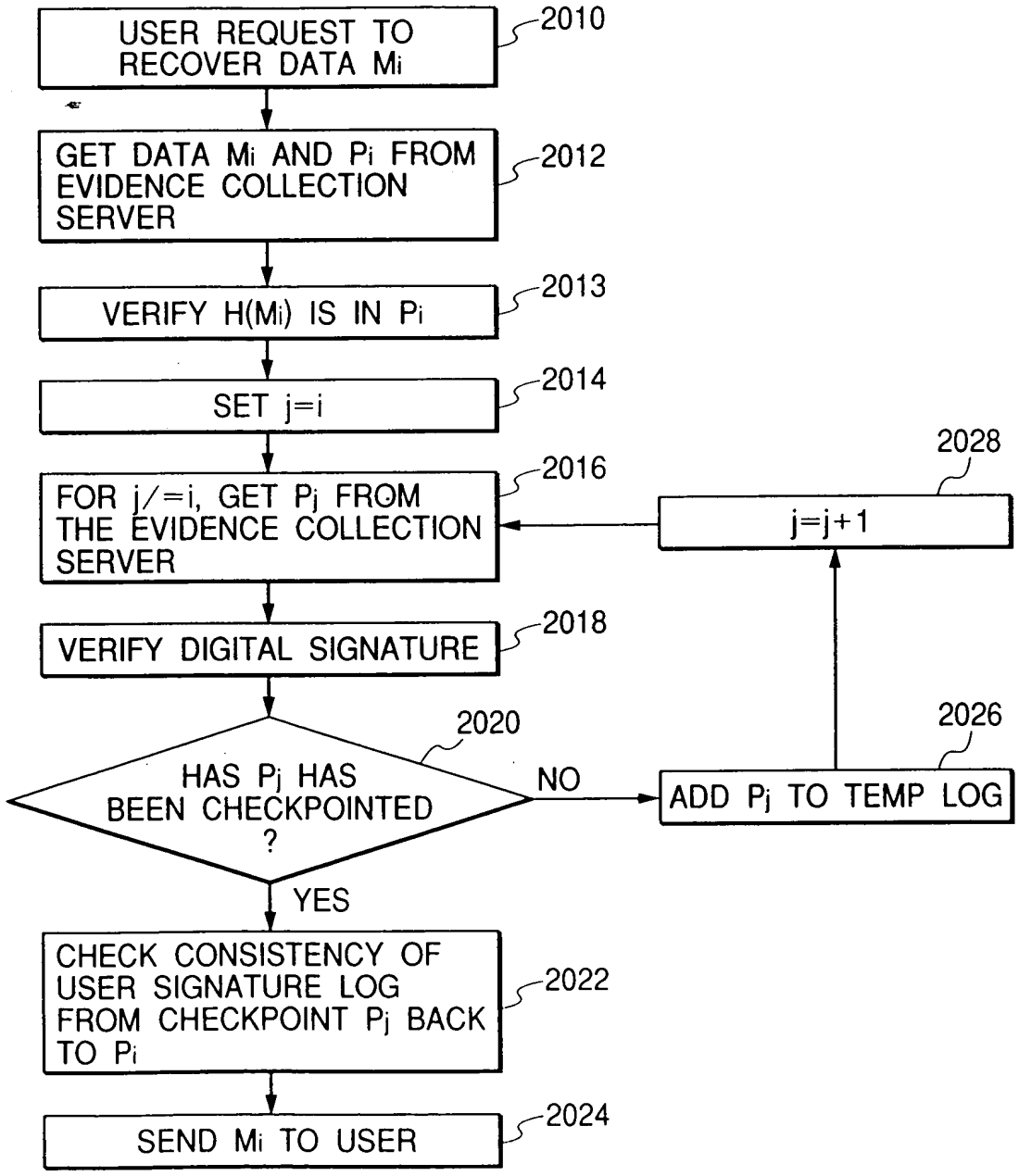
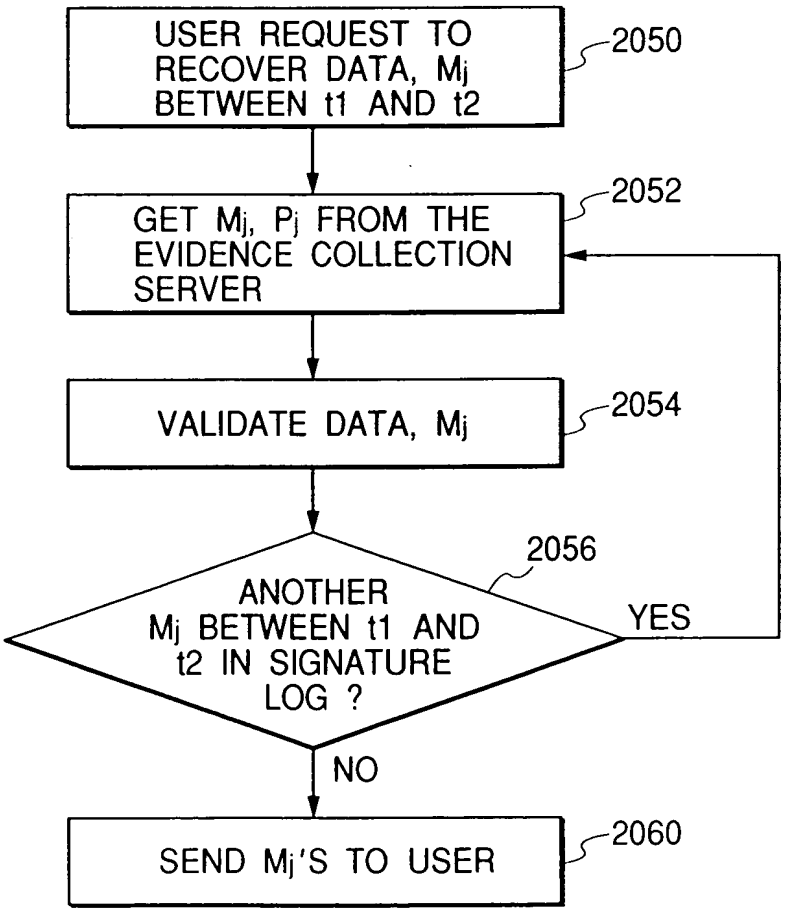


FIG. 20

RECOVERY SERVER RECOVERING USER DATA BETWEEN TWO POINTS IN TIME